

10/069118

PCT/JPOO/05832

日本国特許庁 13.09.00

PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

1999年 8月30日

RECD 06 NOV 2000

WIPO PCT

出願番号  
Application Number:

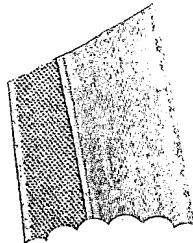
平成11年特許願第243583号

出願人  
Applicant(s):

富士通株式会社  
日本コロムビア株式会社  
三洋電機株式会社

JP00105832

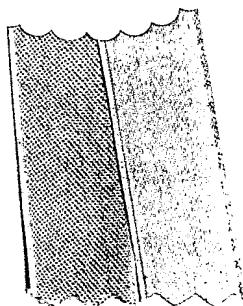
4



PRIORITY  
DOCUMENT

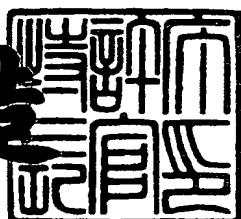
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年10月20日



特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3085321

【書類名】 特許願  
【整理番号】 1990903  
【提出日】 平成11年 8月30日  
【あて先】 特許庁長官殿  
【国際特許分類】 H04M 11/08  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 畑中 正行  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 蒲田 順  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 畠山 卓久  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 長谷部 高行  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 小谷 誠剛  
【発明者】  
【住所又は居所】 東京都港区赤坂四丁目14番14号 日本コロムビア株  
式会社内  
【氏名】 穴澤 健明

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 日置 敏昭

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 金森 美和

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 堀 吉宏

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000004167

【住所又は居所】 東京都港区赤坂四丁目14番14号

【氏名又は名称】 日本コロムビア株式会社

【特許出願人】

【識別番号】 000001889

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号

【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100064746

【弁理士】

【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132

【弁理士】

【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409

【弁理士】

【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ再生装置

【特許請求の範囲】

【請求項1】 暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツキーを復号するための第1の復号鍵を保持する第1の鍵保持部と、

前記データ格納部からの前記暗号化コンテンツキーを基にして、前記第1の鍵保持部からの出力により復号処理を行なうことで、前記コンテンツキーを抽出する第1の復号処理部と、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、前記第1の復号処理部の出力により復号してコンテンツデータを抽出するための第2の復号処理部を含む、データ再生装置。

【請求項2】 前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスする毎に更新される第1のセッションキーを生成する第1のセッションキー発生部と、

前記第1のセッションキーを前記データ格納部にて復号可能な第1の暗号鍵で暗号化して前記データ格納部に与えるための第1の暗号化処理部と、

前記第1のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第1のセッションキーについて復号して前記第1の復号処理部に与える第3の復号処理部をさらに含む、請求項1記載のデータ再生装置。

【請求項3】 前記データ再生部は、前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに異なる第2のセッションキーを、さらに、前記第1の復号鍵により復号可能な暗号化を施して供給を受け、前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに更新される第1のセッションキーを生成する第1のセッションキー発生部と、

前記第1のセッションキーを、外部から入力されたデータから前記第1の複合鍵に基づいて前記第1の復号処理部にて抽出された前記第2のセッションキーで暗号化して前記データ格納部に与えるための第2の暗号処理部と、

前記第1のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第1のセッションキーについて復号して前記第1の復号処理部に与える第3の復号処理部をさらに含む、請求項1記載のデータ再生装置。

【請求項4】 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む、請求項1～3のいずれか1項に記載のデータ再生装置。

【請求項5】 前記データ格納部は、

前記データ格納部に与えられるデータを保持するための記憶部と、

前記第1の暗号化鍵を保持する第2の鍵保持部と、

前記第1の暗号化鍵により暗号化されたデータを復号するための第2の復号鍵を保持するための第3の鍵保持部と、

前記第2の復号鍵に基づいて、前記データ再生部から前記第1の暗号化鍵により暗号化されて伝達された前記第1のセッションキーを復号するための第4の復号処理部と、

前記第4の復号処理部で抽出された前記第1のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第2の暗号化処理部を備える、請求項2記載のデータ再生装置。

【請求項6】 前記データ格納部は、

前記データ格納部に与えられるデータを保持するための記録部と、

前記暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第2のセッションキーを発生する第2のセッションキー発生部と、

前記第1の復号鍵にて復号可能な第2の暗号化鍵により、暗号化処理を行なう第3の暗号化処理部と、

前記第2のセッションキーに基づいて、前記データ再生部から前記第2のセッションキーにて暗号化されて伝達された前記第1のセッションキーを復号するための第5の復号処理手段と、

前記第5の復号処理手段にて抽出された前記第1のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第4の暗号化処理部を備える、請求項3記載のデータ再生装置。

【請求項7】 前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項5または6記載のデータ再生装置。

【請求項8】 前記データ再生部は、

少なくとも前記第1の鍵保持部と、前記第1の復号処理部と、前記第2の復号処理部とが、第三者には読み出不可能なセキュリティ領域に設けられている、請求項1記載のデータ再生装置。

【請求項9】 前記データ再生部は、第三者には読み出不可能なセキュリティ領域に設けられる、請求項1～4のいずれか1項に記載のデータ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、携帯電話網等のデータ配信システムにより配信された配信データの再生装置に関し、より特定的には、配信されたデータに対する著作権保護を可能とするデータ再生装置に関するものである。

【0002】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【0004】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物情報の配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】

【発明が解決しようとする課題】

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作権情報の配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

【0007】

このような記録装置としては、たとえば、メモリカードのように電気的にデータの書き込みおよび消去が可能な媒体が用いられることになる。

【0008】

さらに、配信データを再生する装置としては、このようなデータの配信を受け

るのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

#### 【0009】

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できないように記録媒体においてセキュリティー対策を施す必要がある。

#### 【0010】

それのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なう際に、再生装置側においてコンテンツデータを外部から自由に読み出すことができるとすると、著作権者の権利保護ならびに正規のユーザ側の権利保護にも支障を来たすことになる。

#### 【0011】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、配信されて記録装置に保持された音楽データ等の著作物データを再生する再生装置において、ユーザ以外の者が無断で当該著作物データに対してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供することである。

#### 【0012】

##### 【課題を解決するための手段】

請求項1記載のデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部と、データ格納部からの出力を受けて、暗号化コンテンツデータを再生するためのデータ再生部とを備え、データ再生部は、データ格納部から読み出された暗号化コンテンツキーを復号するための第1の復号鍵を保持する第1の鍵保持部と、データ格納部からの暗号

化コンテンツキーを基にして、第1の鍵保持部からの出力により復号処理を行なうことで、コンテンツキーを抽出する第1の復号処理部と、データ格納部から読み出された暗号化コンテンツデータを受けて、第1の復号処理部の出力により復号してコンテンツデータを抽出するための第2の復号処理部を含む。

#### 【0013】

請求項2記載のデータ再生装置は、請求項1記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスする毎に更新される第1のセッションキーを生成する第1のセッションキー発生部と、第1のセッションキーをデータ格納部にて復号可能な第1の暗号鍵で暗号化してデータ格納部に与えるための第1の暗号化処理部と、第1のセッションキーでさらに暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、第1のセッションキーについて復号して第1の復号処理部に与える第3の復号処理部をさらに含む。

#### 【0014】

請求項3記載のデータ再生装置は、請求項1記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスするごとに異なる第2のセッションキーを、さらに、第1の復号鍵により復号可能な暗号化を施して供給を受け、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスするごとに更新される第1のセッションキーを生成する第1のセッションキー発生部と、第1のセッションキーを、外部から入力されたデータから第1の複合鍵に基づいて第1の復号処理部にて抽出された第2のセッションキーで暗号化してデータ格納部に与えるための第2の暗号処理部と、第1のセッションキーでさらに暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、第1のセッションキーについて復号して第1の復号処理部に与える第3の復号処理部をさらに含む。

#### 【0015】

請求項4記載のデータ再生装置は、請求項1～3のいずれか1項に記載のデータ再生装置の構成に加えて、コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、データ再生部は、符号化

音楽データから符号化方式に基づいて音楽データを再生する音楽再生部と、再生した音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む。

【0016】

請求項5記載のデータ再生装置は、請求項2記載のデータ再生装置の構成に加えて、データ格納部は、データ格納部に与えられるデータを保持するための記憶部と、第1の暗号化鍵を保持する第2の鍵保持部と、第1の暗号化鍵により暗号化されたデータを復号するための第2の復号鍵を保持するための第3の鍵保持部と、第2の復号鍵に基づいて、データ再生部から第1の暗号化鍵により暗号化されて伝達された第1のセッションキーを復号するための第4の復号処理部と、第4の復号処理部で抽出された第1のセッションキーにより、記憶部に保持されたデータを暗号化して出力するための第2の暗号化処理部を備える。

【0017】

請求項6記載のデータ再生装置は、請求項3記載のデータ再生装置の構成に加えて、データ格納部は、データ格納部に与えられるデータを保持するための記録部と、暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第2のセッションキーを発生する第2のセッションキー発生部と、第1の復号鍵にて復号可能な第2の暗号化鍵により、暗号化処理を行なう第3の暗号化処理部と、第2のセッションキーに基づいて、データ再生部から第2のセッションキーにて暗号化されて伝達された第1のセッションキーを復号するための第5の復号処理手段と、第5の復号処理手段にて抽出された第1のセッションキーにより、記憶部に保持されたデータを暗号化して出力するための第4の暗号化処理部を備える。

【0018】

請求項7記載のデータ再生装置は、請求項5または6記載のデータ再生装置の構成に加えて、データ格納部は、データ再生部に対して着脱可能なメモリカードである。

【0019】

請求項8記載のデータ再生装置は、請求項1記載のデータ再生装置の構成に加

えて、データ再生部は、少なくとも第1の鍵保持部と、第1の復号処理部と、第2の復号処理部とが、第三者には読み出不可能なセキュリティ領域に設けられている。

#### 【0020】

請求項9記載のデータ再生装置は、請求項1～4のいずれか1項に記載のデータ再生装置の構成に加えて、データ再生部は、第三者には読み出不可能なセキュリティ領域に設けられる。

#### 【0021】

##### 【発明の実施の形態】

###### 【実施の形態1】

###### 【システムの全体構成】

図1は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

#### 【0022】

なお、以下では携帯電話網を介して、暗号化された音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、暗号化された他の著作物情報データ、例えば画像データ等の著作物情報データを、復号して平文化して再生することが可能なものである。

#### 【0023】

図1を参照して、著作権の存在する音楽情報を管理する配信サーバ10は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリアである携帯電話会社20に、このような暗号化データを与える。

#### 【0024】

携帯電話会社20は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。配信サーバ10は、配線リクエストがあると、要求された暗号化音楽情報を携帯電話会社20の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

**【0025】**

さらに、たとえばユーザ1は、携帯電話100に接続したヘッドホン140等を介してこのような再生された音楽データを聴取することが可能である。

**【0026】**

以下では、このような配信サーバ10と配信キャリア（携帯電話会社）20とを併せて、音楽サーバ30と総称することにする。

**【0027】**

また、このような音楽サーバ30から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

**【0028】**

しかも、配信キャリア20において、たとえば1曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

**【0029】**

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

**【0030】****【配信サーバ10の構成】**

図1において配信サーバ10は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したコンテンツデータやコンテンツキー等の配信情報を保持するための配信情報データベース304と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース302と、暗号化コンテンツデータを復号するためのコンテンツキーKcを公開暗号化キーKpににより暗号化するためのコンテンツキー暗号化処理部316と、配信情報データベース304および課金データベース302からのデータをデータバスBS1を介して受取り、配信サーバ10の動作を制御するためのコントローラ312と、通

信網を介して、配信サーバ10と配信キャリア20との間でデータ授受を行なうための通信装置350とを備える。

#### 【0031】

すなわち、配信情報データベース304からは、コンテンツデータDcが、共通暗号鍵であるコンテンツキーKcにより暗号化したデータ[Dc]Kcと、コンテンツキーKcとが出力される。コントローラ312は、コンテンツキー暗号化処理部316を制御して、このコンテンツキーKcを公開暗号化キーKPpにより暗号化した[Kc]Kpを通信装置350を介して、配信キャリア20に与える。

#### 【0032】

ここで、[Y]Xという表記は、データYを、鍵データXにより復号可能な暗号に変換した情報であることを示している。

#### 【0033】

##### 【端末（携帯電話機）の構成】

図2は、図1に示した携帯電話100の構成を説明するための概略ブロック図である。

#### 【0034】

携帯電話100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話100の各部のデータ授受を行なうためのデータバスBS2と、データバスBS2を介して携帯電話100の動作を制御するためのコントローラ1106と、外部からの指示を携帯電話100に与えるためのタッチキーやダイヤルキーなどを含むキーボード1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるためのディスプレイ1110と、通常の通話動作において、データバスBS2を介して与えられる受信データに基づいて音声を再生するための音声再生部1112とを備える。

#### 【0035】

携帯電話100は、さらに、サーバ30からの暗号化コンテンツデータ[Dc]

] K<sub>c</sub> および暗号化されたコンテンツキー [K<sub>c</sub>] K<sub>p</sub> を格納するためのメモリ 110 と、音楽再生モジュール 1500 とを備える。この音楽再生モジュール 1500 は、公開暗号化キー K<sub>Pp</sub> に対応し、キー K<sub>Pp</sub> で暗号化されたデータを復号可能な秘密復号キー K<sub>p</sub> を保持する K<sub>p</sub> 保持部 1540 と、音楽サーバ 30 から伝送され公開暗号化キー K<sub>Pp</sub> により暗号化されたコンテンツキー [K<sub>c</sub>] K<sub>p</sub> をメモリ 110 から受けて復号するための復号処理部 1530 と、音楽サーバ 30 から配信されメモリ 110 中に格納された暗号化コンテンツデータ [D<sub>c</sub>] K<sub>c</sub> を、復号処理部 1530 で復号抽出されたコンテンツキー K<sub>c</sub> に基づいて復号するための復号処理部 1520 と、復号処理部 1520 からの復号されたコンテンツデータを受けて、コンテンツデータを符号化した符号化方式、例えば MP3、AC3 等のデジタル圧縮符号化方式の再生手順に従って音楽データを再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 を含む。

#### 【0036】

携帯電話機 100 は、さらに、デジタルアナログ変換部 1512 の出力を受けて、ヘッドホン 140 と接続するための接続端子 1514 とを含む。

#### 【0037】

なお、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

#### 【0038】

また、図 2 に示した構成において、音楽再生部 1508、K<sub>p</sub> 保持部 1540、復号処理部 1530 および復号処理部 1520 を、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読み出を不能化するためのモジュール T RM に組み込む構成とすることが可能である。このようなモジュールは、一般に

はタンパーレジスタンスマジュール (Tamper Resistance Module) と呼ばれる。

#### 【0039】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機100の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

#### 【0040】

さらに、図2において実線で囲んだ領域に相当する音楽再生モジュール150を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

#### 【0041】

##### 【再生処理】

図3は、携帯電話100内において、メモリ110に保持された暗号化コンテンツデータから、コンテンツデータを復号して、音楽として外部に出力するための再生処理を説明するフローチャートである。

#### 【0042】

図3を参照して、携帯電話のキーボード1108等からのユーザの指示により、再生リクエストがコントローラ1106に与えられる（ステップS100）。

#### 【0043】

この再生リクエストに応じて、コントローラ1106は、メモリ110を制御して暗号化されたコンテンツキー[Kc]Kpを読み出す（ステップS102）。

。

#### 【0044】

つづいて、復号処理部1530は、メモリ110から読み出された暗号化されたコンテンツキー[Kc]Kpに対する復号処理を行なう（ステップS104）。

。

#### 【0045】

復号処理部1530においてコンテンツキーKcを復号抽出可能な場合は、処理は次のステップに移行し、一方、復号不能と判断された場合は、処理は終了す

る（ステップS110）。

#### 【0046】

復号処理部1530においてコンテンツキーKcを復号抽出可能な場合は、コントローラ1108は、メモリ110を制御して、暗号化コンテンツデータ[Dc]Kcを読み出して、復号処理部1520に与え、復号処理部1520は、復号キーKcにより復号処理して、平文化したコンテンツデータDcを生成して音楽再生部1508に与える。音楽再生部1508により再生された音楽信号は、混合部1510を経由して、デジタルアナログ変換器1512によりアナログ信号に変換されて接続端子1514から外部に出力される。

#### 【0047】

以上のような構成とすることで、再生装置である携帯電話機100内のメモリ110には、暗号化されたコンテンツデータと暗号化されたコンテンツキーが保持されているのみであるため、外部からこのメモリ110内の記憶内容を仮に読み出したとしても、音楽を再生することはできない。

#### 【0048】

しかも、メモリ110から復号処理部1520および1530に与えられるデータも、このような暗号化されたデータであるため、データバスBS2上の信号を外部から仮に検出したとしても、音楽を再生することはできない。

#### 【0049】

さらに、平文化された音楽データが伝達される部分は、上述のとおり、タンパーケジスタンスマジュールで構成されているので、この部分から音楽データを外部に読み出すこともできない構成となっている。

#### 【0050】

したがって、図2に示した携帯電話機100の構成により、ユーザ以外の者が無断でコンテンツデータに対してアクセスを行なうことから保護することが可能となる。

#### 【0051】

##### 【実施の形態2】

図4は、本発明の実施の形態2の携帯電話機200の構成を説明するための概

略ブロック図であり、実施の形態1の図2と対比される図である。

【0052】

図2に示した携帯電話機100の構成と、携帯電話機200の構成が異なる点は、以下のとおりである。

【0053】

まず、図4においては、携帯電話機200には、携帯電話機200により受信された暗号化された音楽データを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機200中の音楽再生モジュール1500に与えるための着脱可能なメモリカード120が装着される構成となっている。これに応じて、携帯電話機200は、メモリカード120とデータバスBS2との間のデータの授受を制御するためのメモリインターフェース1200をさらに備えている。

【0054】

さらに、携帯電話機200の構成では、音楽再生モジュール1500の構成も、携帯電話機100の構成と異なる。

【0055】

すなわち、携帯電話機200の音楽再生モジュール1500は、メモリカード120と携帯電話の他の部分とのデータ授受にあたり、データバスBS2上においてやり取りされるデータを暗号化するための後に説明するセッションキーK<sub>s</sub>を乱数等により発生するセッションキー発生部1502と、セッションキー発生部1502により生成されたセッションキーK<sub>s</sub>を暗号化して、データバスBS2に与えるための暗号化処理部1504と、データバスBS2によりメモリカード120から伝送され、公開暗号鍵K<sub>P</sub><sub>p</sub>およびセッションキーK<sub>s</sub>により暗号化されたコンテンツキーをセッションキーK<sub>s</sub>について復号して出力する復号処理部1506と、公開暗号化キーK<sub>P</sub><sub>p</sub>に対応し、キーK<sub>P</sub><sub>p</sub>で暗号化されたデータを復号可能な秘密復号キーK<sub>P</sub>を保持するK<sub>P</sub>保持部1540と、復号処理部1506の出力を受けて、メモリカード120から伝送され公開暗号化キーK<sub>P</sub><sub>p</sub>により暗号化されたコンテンツキー[K<sub>c</sub>]K<sub>P</sub>を復号するための復号処理部1530と、サーバ30から配信されメモリカード120中に格納された暗号

化コンテンツデータ [Dc] Kc を、復号処理部 1530 で復号抽出されたコンテンツキー Kc に基づいて復号するための復号処理部 1520 と、復号処理部 1520 からの復号されたコンテンツデータ Dc を受けて、音楽サーバ 30 から配信された音楽データを再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 とを含む。

#### 【0056】

携帯電話機 200 のその他の部分は、実施の形態 1 の携帯電話機 100 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

#### 【0057】

なお、図 4 においても、説明の簡素化のため本発明の音楽データの配信に関するブロックのみを記載し、形態電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

#### 【0058】

また、図 4 に示した構成において、音楽再生部 1508、Kp 保持部 1540、復号処理部 1530、復号処理部 1520、復号処理部 1506、暗号化処理部 1504 および Ks 発生部 1502 を、TRM に組み込む構成とすることが可能である。

#### 【0059】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機 200 の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

#### 【0060】

さらに、図 4 において実線で囲んだ領域に相当する音楽再生モジュール 1500 を、TRM とすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

**【0061】****[暗号／復号キーの構成]**

図5は、図4に示した携帯電話機200において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

**【0062】**

まず、図4に示した構成において、メモリカード120内のデータ処理を管理するための鍵としては、メモリカードに固有な公開暗号化鍵K<sub>Pm</sub>と、公開暗号化鍵K<sub>Pm</sub>により暗号化されたデータを復号するためのキーK<sub>Pm</sub>とは非対称な秘密復号鍵K<sub>m</sub>とがある。

**【0063】**

ここで、キーK<sub>Pm</sub>とキーK<sub>m</sub>とが非対称とは、複数の公開暗号化キーK<sub>Pm</sub>により暗号化されたデータが同一の復号キーK<sub>m</sub>により復号できることを意味する。

**【0064】**

したがって、メモリカード120と携帯電話200とのセッションキーの授受にあたっては、後に説明するようにこれら暗号鍵K<sub>m</sub>、復号鍵K<sub>Pm</sub>が用いられることになる。

**【0065】**

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、携帯電話機という再生装置に固有な公開暗号化キーをK<sub>Pp</sub>と、音楽再生モジュール管理の鍵として、このキーK<sub>Pp</sub>で暗号化されたデータを復号化でき、キーK<sub>Pp</sub>とは非対称な秘密復号キーK<sub>p</sub>と、各通信ごとにK<sub>s</sub>発生器1502において生成される共通鍵K<sub>s</sub>とが用いられる。

**【0066】**

ここで、共通鍵K<sub>s</sub>は、たとえば、携帯電話機200とメモリカード120との間のコンテンツデータの授受のためのアクセスが行なわれるごとにK<sub>s</sub>発生器1502において発生する。

**【0067】**

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と

呼ぶことにし、共通鍵K<sub>s</sub>を「セッションキー」とも呼ぶことにする。

#### 【0068】

したがって、共通鍵K<sub>s</sub>は各通信セッションに固有の値を有することになり、音楽再生モジュール1500において管理される。

#### 【0069】

さらに、メモリカード120に記録される著作権情報データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツキーK<sub>c</sub>があり、この共通鍵K<sub>c</sub>により暗号化されたコンテンツデータが復号（平文化）されるものとする。

#### 【0070】

著作権の存在するコンテンツデータD<sub>c</sub>は、上述のとおり、たとえば音楽データであり、このコンテンツデータをコンテンツキーK<sub>c</sub>で復号化可能なデータを、暗号化コンテンツデータ[D<sub>c</sub>]K<sub>c</sub>と呼ぶ。

#### 【0071】

また、配信サーバ10から携帯電話機200に向けて、コンテンツキーK<sub>c</sub>が配信される場合には、このコンテンツキーK<sub>c</sub>は、すくなくとも公開暗号化キーK<sub>P</sub><sub>p</sub>により暗号化されており、メモリカード120中には、この暗号化コンテンツキー[K<sub>c</sub>]K<sub>p</sub>として格納されているものとする。

#### 【0072】

##### 〔メモリカードの構成〕

図6は、図4に示したメモリカード120の構成を説明するための概略ブロック図である。

#### 【0073】

メモリカード120は、メモリインターフェース1200との間で信号を端子1202を介して授受するデータバスBS3と、公開暗号化キーK<sub>P</sub><sub>m</sub>の値を保持し、データバスBS3に公開暗号化キーK<sub>P</sub><sub>m</sub>を出力するためのK<sub>P</sub><sub>m</sub>保持部1401と、カード120に対応する秘密復号鍵K<sub>m</sub>を保持するためのK<sub>m</sub>保持部1402と、データバスBS3にメモリインターフェース1200から与えられるデータから、秘密復号鍵K<sub>m</sub>により復号処理をすることにより、セッションキー

$K_s$  を抽出する復号処理部 1404 と、データバス BS3 から、公開暗号化キー  $K_p$  で暗号化されているコンテンツキー  $K_c$  およびコンテンツキー  $K_c$  により暗号化されている暗号化コンテンツデータ [Dc]  $K_c$  を受けて格納するためのメモリ 1412 と、復号処理部 1404 により抽出されたセッションキー  $K_s$  に基づいて、メモリ 1412 からの出力を暗号化してデータバス BS3 に与えるための暗号化処理部 1406 と、メモリカード 120 の動作を制御するためのコントローラ 1420 とを備える。

#### 【0074】

なお、図6のメモリカード 120 内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール TRM に組込まれる構成とすることも可能である。

#### 【0075】

##### 【再生処理】

図7は、携帯電話機 200 内において、メモリカード 120 に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

#### 【0076】

図7を参照して、携帯電話のキーボード 1108 等からのユーザの指示により、再生リクエストがメモリカード 120 に対して出力される（ステップ S200）。

#### 【0077】

メモリカード 120においては、この再生リクエストに応じて、コントローラ 1420 は、 $K_{Pm}$  保持部 1401 から、データバス BS3、端子 1202 およびメモリインターフェース 1200 を介して、公開暗号化キー  $K_{Pm}$  を携帯電話 200 に対して送信する（ステップ S202）。

#### 【0078】

携帯電話機 200 では、カード 120 からのキー  $K_{Pm}$  を受信すると（ステップ S204）、 $K_s$  発生部 1502 においてセッションキー  $K_s$  を生成し（ステ

ップS206)、暗号化処理部1504が、キーK<sub>Pm</sub>により、セッションキーK<sub>s</sub>を暗号化してデータ[K<sub>s</sub>]K<sub>Pm</sub>を生成し、データバスBS2を通して、カード120に対して送信する(ステップS208)。

【0079】

メモリカード120は、携帯電話機200により生成され、かつ暗号化されたセッションキーK<sub>s</sub>を受け取り、復号処理部1404において秘密復号キーK<sub>m</sub>により復号し、セッションキーK<sub>s</sub>を抽出する(ステップS210)。

【0080】

続いて、メモリカード120は、メモリ1412から、暗号化されているデータ[K<sub>c</sub>]K<sub>p</sub>を読出す(ステップS212)。

【0081】

続いて、メモリカード120は、暗号化処理部1406において抽出したセッションキーK<sub>s</sub>により、暗号化コンテンツキー[[K<sub>c</sub>]K<sub>p</sub>]K<sub>s</sub>を暗号化し、暗号化された暗号化コンテンツキー[[K<sub>c</sub>]K<sub>p</sub>]K<sub>s</sub>をデータバスBS2に与える(ステップS214)。

【0082】

携帯電話機200の復号処理部1506は、メモリカード120から送信された暗号化された暗号化コンテンツキー[[K<sub>c</sub>]K<sub>p</sub>]K<sub>s</sub>をセッションキーK<sub>s</sub>により復号処理を行なうことにより、暗号化コンテンツキー[K<sub>c</sub>]K<sub>p</sub>を取得する(ステップS216)。

【0083】

さらに、携帯電話機200の復号処理部1530は、K<sub>p</sub>保持部1540からのキーK<sub>p</sub>に基づいて、データ[K<sub>c</sub>]K<sub>p</sub>の復号処理を行なう(ステップS218)。

【0084】

復号処理部1530が復号処理により、コンテンツキーK<sub>c</sub>を抽出できた場合は(ステップS220)、処理は次のステップS222に進み、抽出できない場合は(ステップS220)、処理は終了する(ステップS226)。

【0085】

復号処理部1530が復号処理により、コンテンツキーKcを抽出できた場合は、メモリカード120は、暗号化されたコンテンツデータ[Dc]Kcをメモリ1412から読み出し、データバスBS2に与える（ステップS222）。

#### 【0086】

携帯電話機200の復号処理部1520は、暗号化されたコンテンツデータ[Dc]Kcを、抽出されたコンテンツキーKcにより復号処理して平文の音楽データDcを生成し、音楽再生部1508は、コンテンツデータDcを再生して混合部1510に与える。デジタルアナログ変換部1512は、混合部1510からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップS226）。

#### 【0087】

このような構成とすることで、携帯電話機200において生成されたセッションキーに基づいてコンテンツキーを暗号化した上で、メモリカード120から携帯電話機200に送信して再生動作を行なうことが可能となる。

#### 【0088】

以上のような構成により、実施の形態1の携帯電話機100の奏する効果に加えて、実施の形態2の形携帯電話機200においては、携帯電話機200に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

#### 【0089】

しかも、携帯電話機とメモリカードとの間のデータの授受は、セッションキーにより暗号化された上で行なわれる所以、データに対するセキュリティーが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

#### 【0090】

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することでも、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

#### 【0091】

## 〔実施の形態3〕

図8は、本発明の実施の形態3の携帯電話機300の構成を説明するための概略ブロック図であり、実施の形態2の図4と対比される図である。

## 【0092】

図8に示した実施の形態3の携帯電話機300の構成と、実施の形態2の携帯電話機200の構成が異なる点は、以下のとおりである。

## 【0093】

まず、図8においては、携帯電話機300には、携帯電話機300により受信された暗号化された音楽データを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機300中の音楽再生モジュール1500に与えるための着脱可能なメモリカード130が装着される構成となっている。

## 【0094】

メモリカード130は、後に説明するように、メモリカード130自身でセッションキーK<sub>s</sub>2を生成する点で、メモリカード120と異なる。

## 【0095】

さらに、携帯電話機300の構成では、音楽再生モジュール1500の構成も、携帯電話機200の構成と異なる。

## 【0096】

すなわち、携帯電話機300の音楽再生モジュール1500は、メモリカード130と携帯電話の他の部分とのデータ授受にあたり、データバスB<sub>S</sub>2上においてやり取りされるデータを暗号化するためのセッションキーK<sub>s</sub>1を乱数等により発生するセッションキー発生部1552と、セッションキー発生部1552により生成されたセッションキーK<sub>s</sub>1をメモリカード130からのセッションキーK<sub>s</sub>2で暗号化して、データバスB<sub>S</sub>2に与えるための暗号化処理部1554と、データバスB<sub>S</sub>2によりメモリカード130から伝送され、公開暗号鍵K<sub>Pp</sub>およびセッションキーK<sub>s</sub>1により暗号化されたコンテンツキーK<sub>c</sub>をセッションキーK<sub>s</sub>1について復号して出力する復号処理部1556と、コントローラ1106により制御されて、データバスB<sub>S</sub>2により伝達された暗号化された

メモリカード130のセッションキー[Ks2]Kpまたは復号処理部1556から出力された暗号化コンテンツキー[Kc]Kpのいずれかを、公開暗号化鍵Kpにより暗号化されたデータを復号するための復号処理部1530に与える切換え回路1550とを含む。

#### 【0097】

暗号化処理部1554は、復号処理部1530において秘密復号鍵Kpにより復号されて抽出されたメモリカード130のセッションキーKs2を受けて、セッションキー発生部1552により生成されたセッションキーKs1をセッションキーKs2で暗号化処理する。

#### 【0098】

携帯電話機300のその他の部分は、実施の形態2の携帯電話機200の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

#### 【0099】

なお、図8においても、説明の簡素化のため本発明の音楽データの配信に関するブロックのみを記載し、形態電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

#### 【0100】

また、図8に示した構成において、音楽再生部1508、Kp保持部1540、復号処理部1530、復号処理部1520、復号処理部1556、暗号化処理部1554、セッションキー発生部1552および切換え回路1550を、TRMに組み込む構成とすることが可能である。

#### 【0101】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機300の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

#### 【0102】

さらに、図8において実線で囲んだ領域に相当する音楽再生モジュール1500を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが

可能である。

#### 【0103】

##### 〔暗号／復号キーの構成〕

図9は、図8に示した携帯電話機300において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

#### 【0104】

まず、図8に示した構成において、メモリカード130内のデータ処理を管理するための鍵としては、メモリカードに固有な公開暗号化鍵K<sub>Pm</sub>と、公開暗号化鍵K<sub>Pm</sub>により暗号化されたデータを復号するためのキーK<sub>Pm</sub>とは非対称な秘密復号鍵K<sub>m</sub>と、メモリカード130が生成し各セッションに固有なセッションキーK<sub>s2</sub>がある。

#### 【0105】

したがって、メモリカード130と携帯電話300とのセッションキーの授受にあたっては、後に説明するようにこれら暗号鍵K<sub>m</sub>、復号鍵K<sub>Pm</sub>、セッションキーK<sub>s2</sub>が用いられることになる。

#### 【0106】

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、携帯電話機という再生装置に固有な公開暗号化キーであって、コンテンツデータの配信時にコンテンツデータとともに配信され、後に説明するようにメモリカード130内に記憶される公開暗号鍵K<sub>Pp</sub>と、音楽再生モジュールの管理の鍵として、このキーK<sub>Pp</sub>で暗号化されたデータを復号化でき、キーK<sub>Pp</sub>とは非対称な秘密復号キーK<sub>p</sub>と、各アクセスごとにセッションキー発生器1552において生成される共通鍵（セッションキー）K<sub>s1</sub>とが用いられる。

#### 【0107】

共通鍵K<sub>s1</sub>も各通信セッションに固有の値を有することになり、音楽再生モジュール1500において管理される。

#### 【0108】

さらに、メモリカード130に記録される著作権情報データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテ

ンツキーK<sub>c</sub>があり、この共通鍵K<sub>c</sub>により暗号化されたコンテンツデータが復号（平文化）されるものとする。

#### 【0109】

また、配信サーバ10から携帯電話機300に向けて、コンテンツキーK<sub>c</sub>が配信される場合には、このコンテンツキーK<sub>c</sub>は、すくなくとも公開暗号化キーK<sub>Pp</sub>により暗号化されており、メモリカード120中には、この暗号化コンテンツキー[K<sub>c</sub>]K<sub>p</sub>として格納されているものとする。

#### 【0110】

さらに、著作権の存在するコンテンツデータD<sub>c</sub>は、このコンテンツデータをコンテンツキーK<sub>c</sub>で復号化可能な暗号化コンテンツデータ[D<sub>c</sub>]K<sub>c</sub>としてメモリカード130に格納されているものとする。

#### 【0111】

##### 【メモリカードの構成】

図10は、図8に示したメモリカード130の構成を説明するための概略ブロック図である。

#### 【0112】

メモリカード130は、メモリインターフェース1200との間で信号を端子1202を介して授受するデータバスBS3と、セッション毎にセッションキーK<sub>s2</sub>を生成するためのセッションキー発生部1450と、セッションキーK<sub>s2</sub>を公開暗号化鍵K<sub>Pp</sub>で暗号化してデータバスBS3に与えるための暗号化処理部1452と、データバスBS3にメモリインターフェース1200から与えられるデータ[K<sub>s1</sub>]K<sub>s2</sub>から、セッションキーK<sub>s2</sub>により復号処理をすることにより、携帯電話機300からのセッションキーK<sub>s1</sub>を抽出する復号処理部1454と、データバスBS3から、公開暗号化鍵K<sub>Pp</sub>と公開暗号化鍵K<sub>Pp</sub>で暗号化されているコンテンツキー[K<sub>c</sub>]K<sub>p</sub>とコンテンツキーK<sub>c</sub>により暗号化されている暗号化コンテンツデータ[D<sub>c</sub>]K<sub>c</sub>との3つを受けて格納するためのメモリ1412と、復号処理部1454により抽出されたセッションキーK<sub>s1</sub>に基づいて、メモリ1412からの出力を暗号化してデータバスBS3に与えるための暗号化処理部1456と、メモリカード130の動作を制御するた

めのコントローラ1420とを備える。

#### 【0113】

なお、図10のメモリカード130内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読み出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

#### 【0114】

##### 【再生処理】

図11は、携帯電話機300内において、メモリカード130に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

#### 【0115】

図11を参照して、携帯電話のキーボード1108等からのユーザの指示により、再生リクエストがメモリカード130に対して出力される（ステップS300）。

#### 【0116】

メモリカード130においては、この再生リクエストに応じて、コントローラ1420は、セッションキー発生部1450を制御してセッションキーKs2を発生させる（ステップS302）。コントローラ1420の制御により、このセッションキーKs2を暗号化処理部1452は公開暗号化鍵Kpにより暗号化して暗号化セッションキー[Ks2]Kpを生成し、この暗号化セッションキー[Ks2]Kpを、データバスBS3、端子1202およびメモリインターフェース1200を介して、携帯電話300に対して送信する（ステップS304）。

#### 【0117】

携帯電話機300では、カード130からの暗号化セッションキー[Ks2]Kpを受信すると、切換え回路1550を介して復号処理部1530が暗号化セッションキー[Ks2]Kpを受けて復号しセッションキーKs2を獲得する（ステップS306）。

## 【0118】

携帯電話機300においては、セッションキー発生部1552においてセッションキーKs1を生成し（ステップS308）、暗号化処理部1554が、ステップS306において抽出されたセッションキーKs2により、セッションキーKs1を暗号化してデータ[Ks1]Ks2を生成し、データバスBS2を介して、カード130に対して送信する（ステップS310）。

## 【0119】

メモリカード130は、携帯電話機300により生成され、かつ暗号化されたセッションキー[Ks1]Ks2を受け取り、復号処理部1454においてセッションキーKs2により復号し、セッションキーKs1を抽出する（ステップS312）。

## 【0120】

続いて、メモリカード130は、メモリ1412から、暗号化されているデータ[Kc]Kpを読出す（ステップS314）。

## 【0121】

続いて、メモリカード130は、暗号化処理部1456において、抽出したセッションキーKs1により、暗号化コンテンツキー[Kc]Kpを暗号化し、暗号化された暗号化コンテンツキー[[Kc]Kp]Ks1をデータバスBS3等を介してデータバスBS2に与える（ステップS316）。

## 【0122】

携帯電話機300の復号処理部1556は、メモリカード130から送信された暗号化された暗号化コンテンツキー[[Kc]Kp]Ks1に対してセッションキーKs1により復号処理を行なうことにより、暗号化コンテンツキー[Kc]Kpを取得する（ステップS318）。

## 【0123】

さらに、携帯電話機300の復号処理部1530は、切換え回路1550を介して暗号化コンテンツキー[Kc]Kpを受け、Kp保持部1540からのキーKpに基づいて、データ[Kc]Kpの復号処理を行なう（ステップS320）。

。

## 【0124】

復号処理部1530が復号処理により、コンテンツキーKcを抽出できた場合は（ステップS322）、処理は次のステップS324に進み、抽出できない場合は（ステップS322）、処理は終了する（ステップS330）。

## 【0125】

復号処理部1530が復号処理により、コンテンツキーKcを抽出できた場合は、メモリカード130は、暗号化されたコンテンツデータ[Dc]Kcをメモリ1412から読み出し、データバスBS3等を介してデータバスBS2に与える（ステップS324）。

## 【0126】

携帯電話機300の復号処理部1520は、暗号化されたコンテンツデータ[Dc]Kcを、抽出されたコンテンツキーKcにより復号処理して平文の音楽データDcを生成し、音楽再生部1508は、コンテンツデータDcを再生して混合部1510に与える。デジタルアナログ変換部1512は、混合部1510からのデータを受け取って変換し、外部に再生された音楽を出力し（ステップS328）、処理が終了する（ステップS330）。

## 【0127】

このような構成とすることで、携帯電話機300において生成されたセッションキーKs1に基づいてコンテンツキーを暗号化した上で、メモリカード130から携帯電話機300に送信して再生動作を行なうことが可能となる。しかも、メモリカード130においてセッション毎に生成されたセッションキーKs2により暗号化した上で、メモリカード130と携帯電話300との間でセッションキーKs1の授受が行なわれる所以、実施の形態2よりも一層、セキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

## 【0128】

また、以上のような構成により、実施の形態3の形携帯電話機300においても、携帯電話機300に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれる

ことがない。

### 【0129】

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することでき、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

### 【0130】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内のすべての変更が含まれることが意図される。

### 【0131】

#### 【発明の効果】

以上説明したとおり、本願発明にかかるデータ再生装置では、正規のユーザがメモリ中に格納したコンテンツデータに対して、第三者が不当に配信データへのアクセスを行なうことが困難な構成となっているので、著作権者および正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

#### 【図面の簡単な説明】

【図1】 本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【図2】 図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【図3】 携帯電話機100内において、暗号化コンテンツデータから音楽情報を復号化するための再生処理を説明するフローチャートである。

【図4】 本発明の実施の形態2の携帯電話機200の構成を説明するための概略ブロック図である。

【図5】 図4に示した携帯電話機200において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図6】 図4に示したメモリカード120の構成を説明するための概略ブ

ロック図である。

【図7】 携帯電話機200において、暗号化コンテンツデータから音楽情報を復号化するための再生処理を説明するフローチャートである。

【図8】 本発明の実施の形態3の携帯電話機300の構成を説明するための概略ブロック図である。

【図9】 図8に示した携帯電話機300において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図10】 図8に示したメモリカード130の構成を説明するための概略ブロック図である。

【図11】 携帯電話機300において、暗号化コンテンツデータから音楽情報を復号化するための再生処理を説明するフローチャートである。

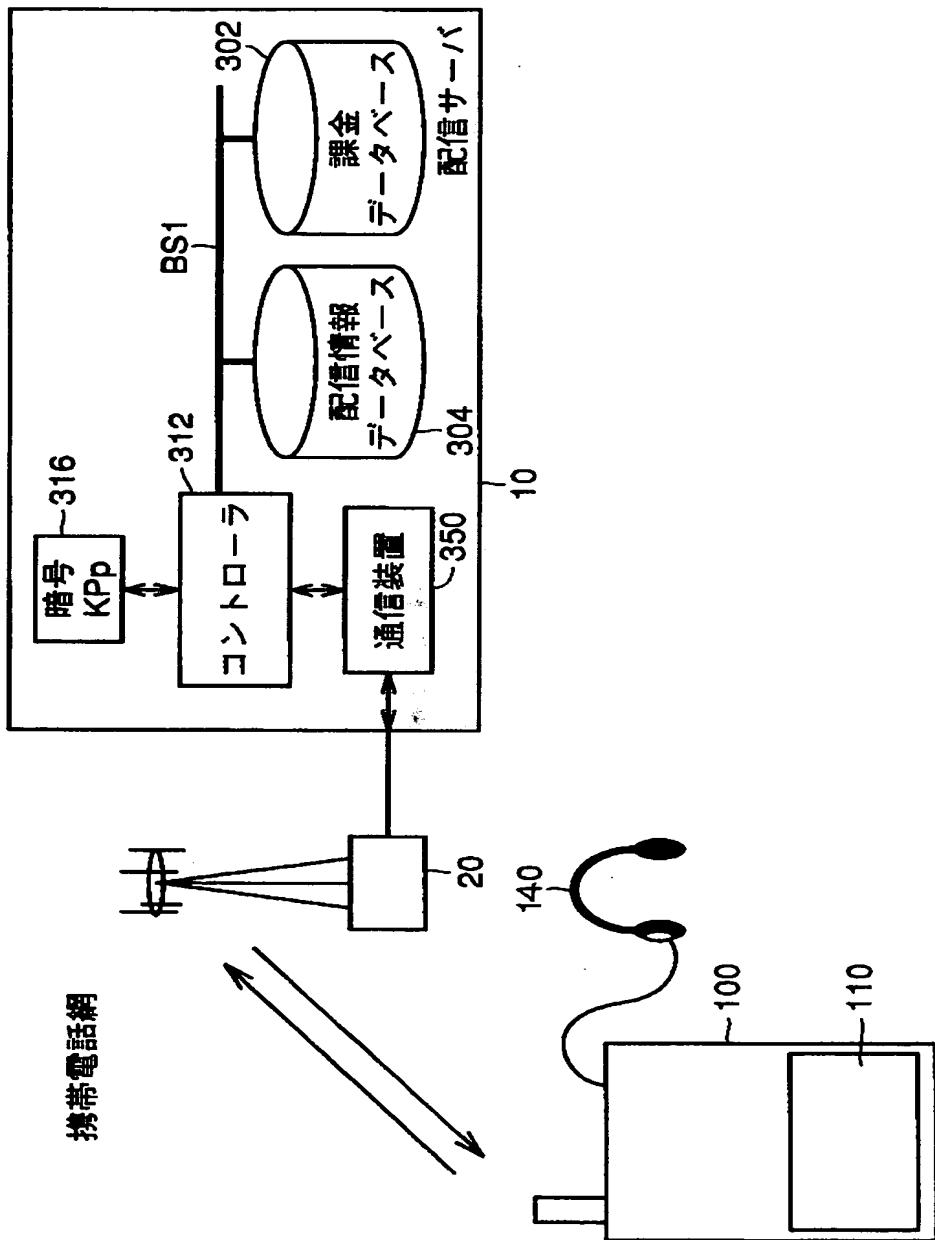
#### 【符号の説明】

10 配信サーバ、20 配信キャリア、30 音楽サーバ、100, 200  
 携帯電話機、110, 120, 130 メモリカード、140 ヘッドホン、  
 1102 アンテナ、1104 送受信機、1106 コントローラ、1108  
 キーボード、1110 ディスプレイ、1112 音声再生部、1200 メ  
 モリインターフェース、1401 KPM保持部、1404 復号処理部、140  
 6 暗号化処理部、1420 コントローラ、1502 セッションキー発生部  
 、1504 暗号化処理部、1506 復号処理部、1508 音楽再生部、1  
 510 混合部、1512 デジタルアナログ変換器。

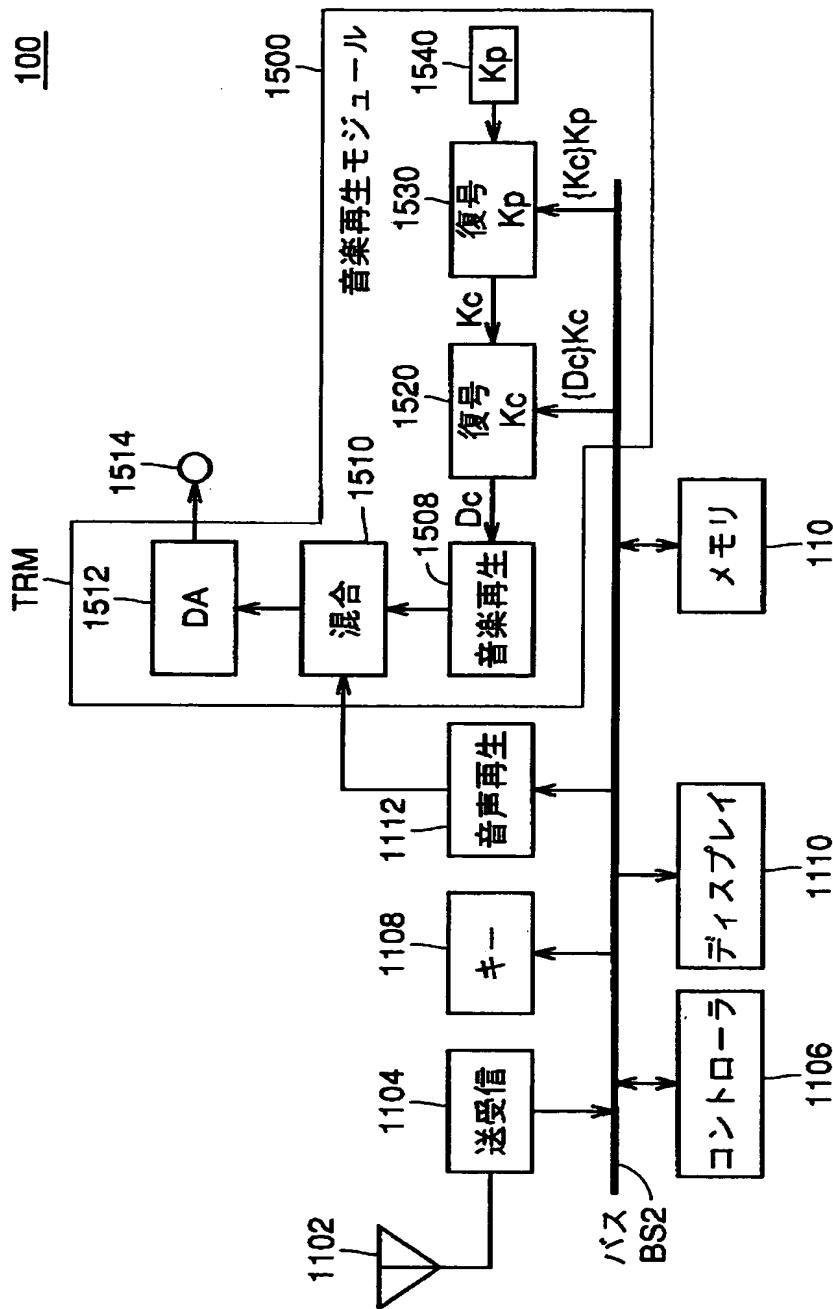
【書類名】

図面

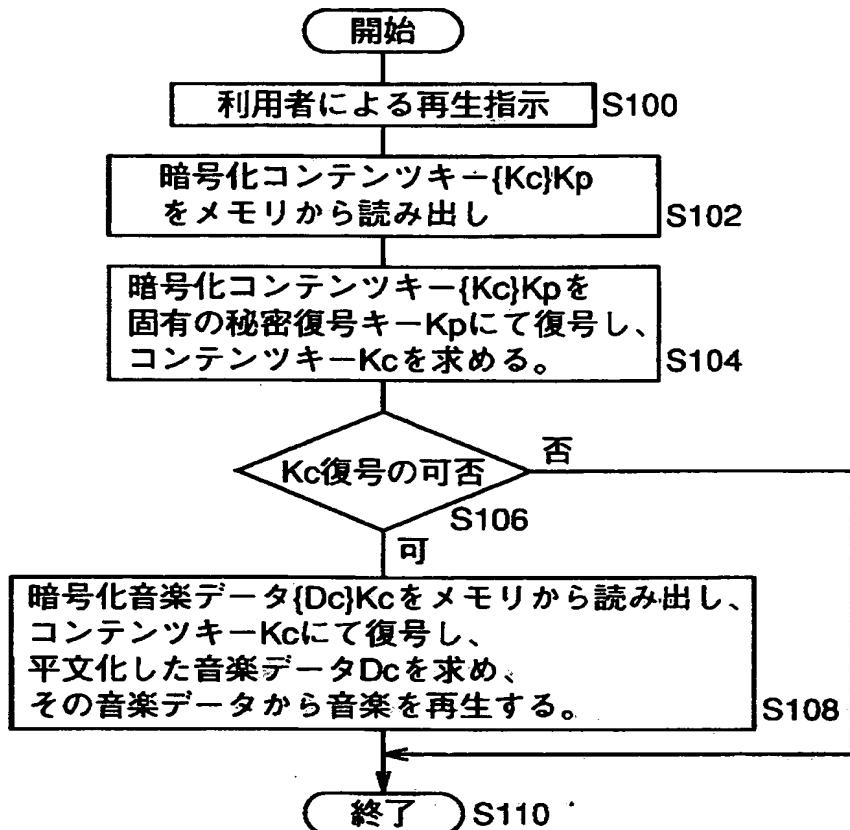
【図1】



【図2】

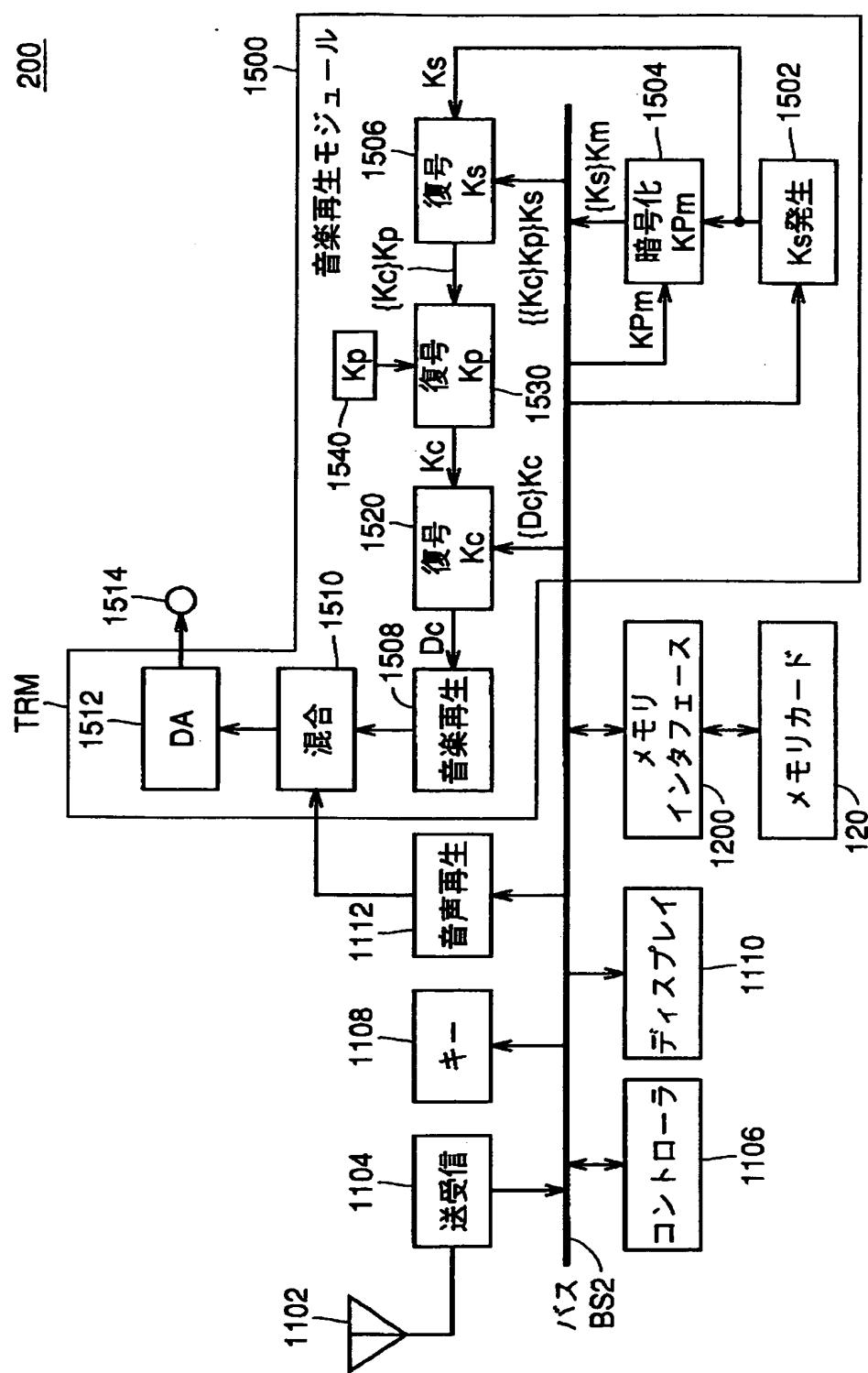


【図3】



【図4】

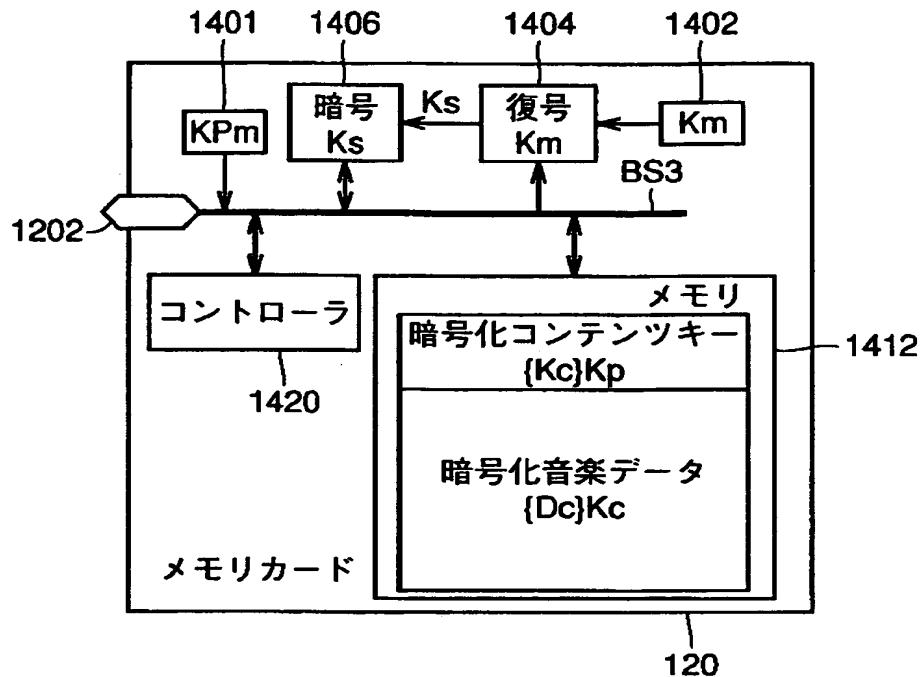
200



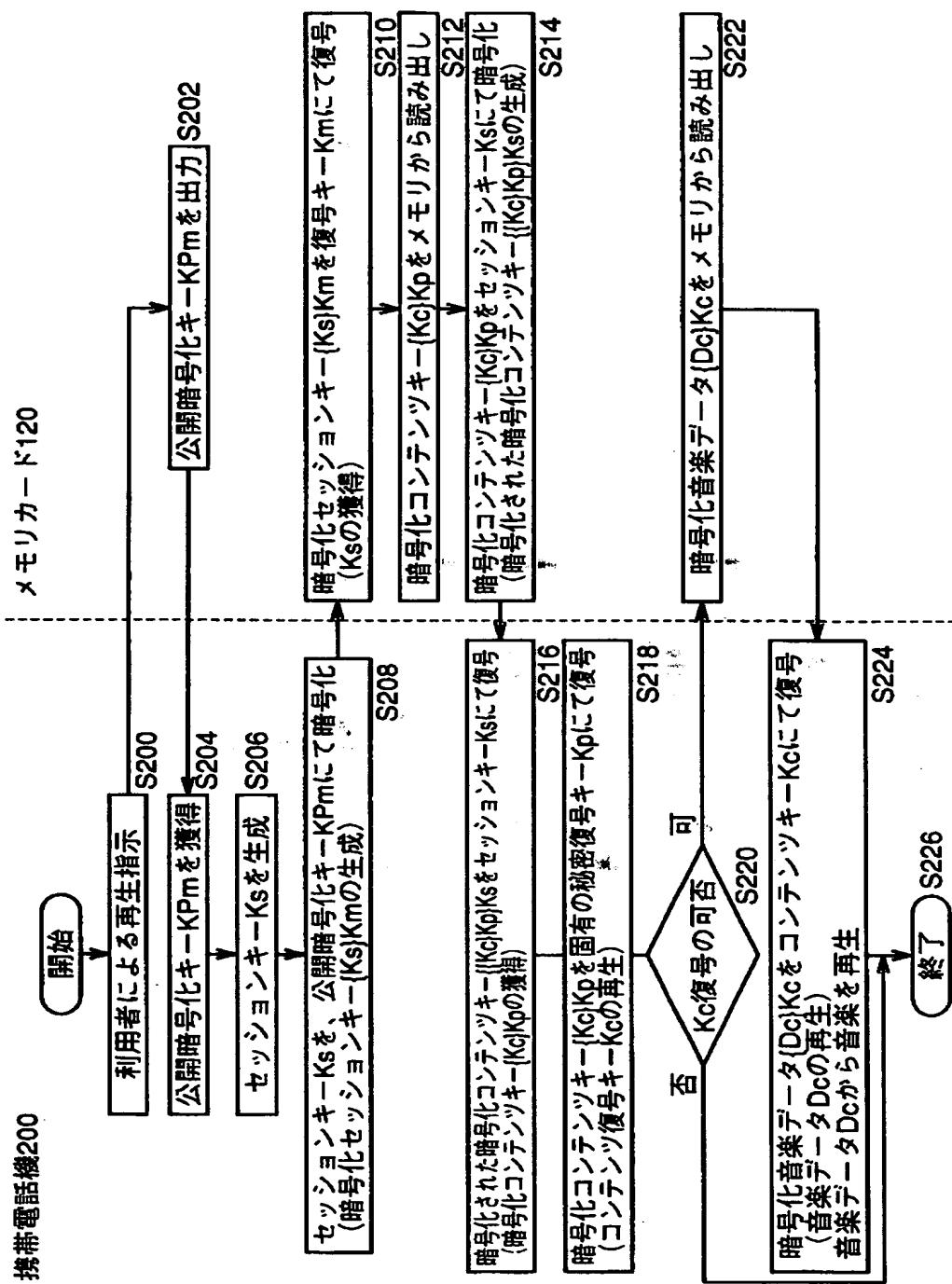
【図5】

	記号	属性	特性
メモリカード 管理の鍵	Km	秘密復号鍵	メモリカード毎に異なる
	KPm	公開暗号鍵	Kmと対を成す KPmで暗号化されたデータは非対称な 復号鍵Kmで復号可能
音楽再生モジュール 管理の鍵	Kp	秘密復号鍵	Kmと対を成す データ再生装置 (携帯電話機) 固有
	Ks	共通鍵	セッション固有 セッション固有 メモリと音楽再生モジュール間 のアクセス毎に発生
配信データ	KPp	公開暗号鍵	Kpと対を成す (KCを暗号化) KPpで暗号化されたデータは非対称な 復号鍵Kpで復号可能
	Kc	共通鍵	コンテンツキー 暗号化コンテンツデータの復号鍵
	Dc	コンテンツ データ	例：音楽データ

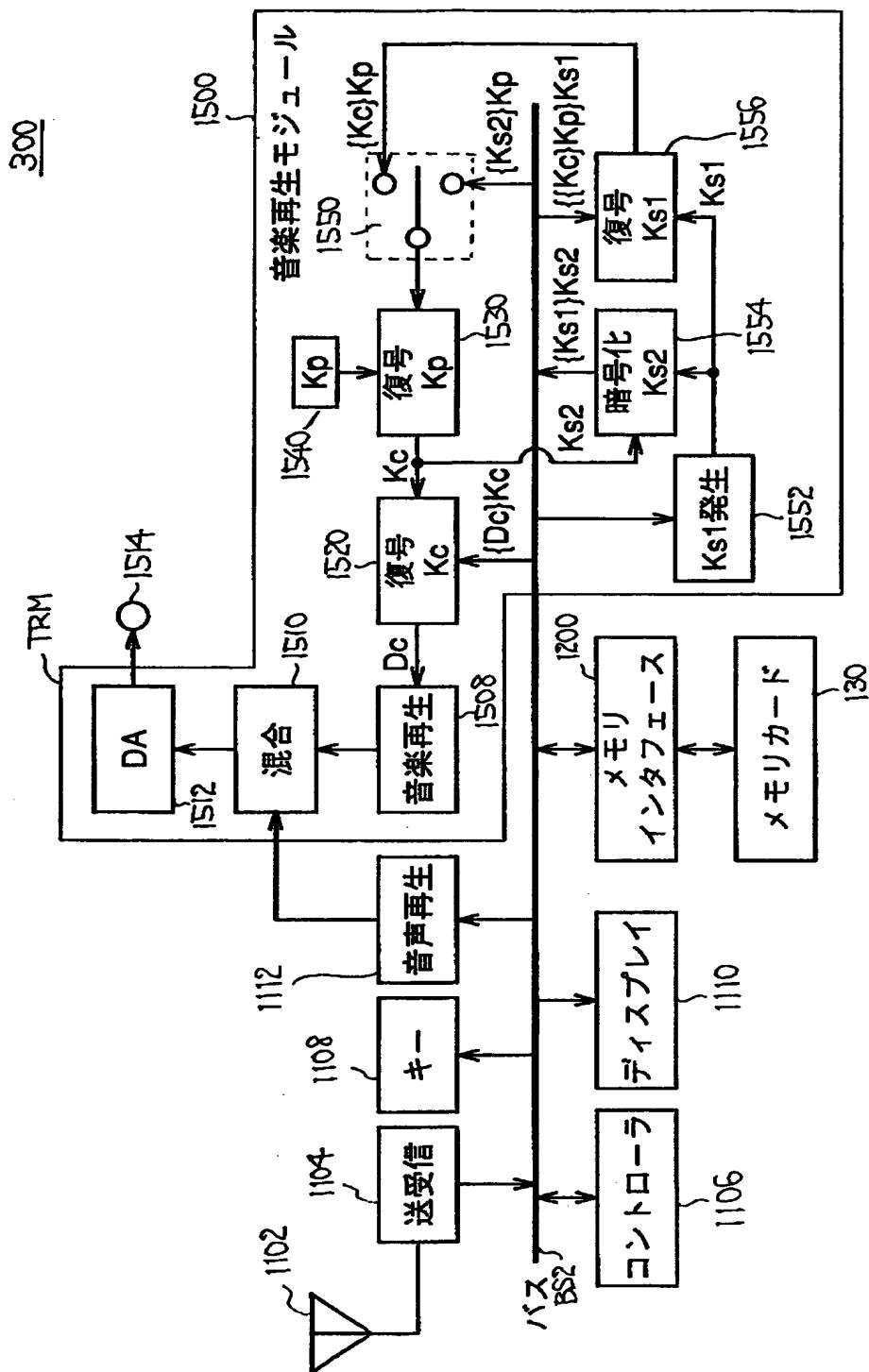
【図6】



【図7】



【図8】

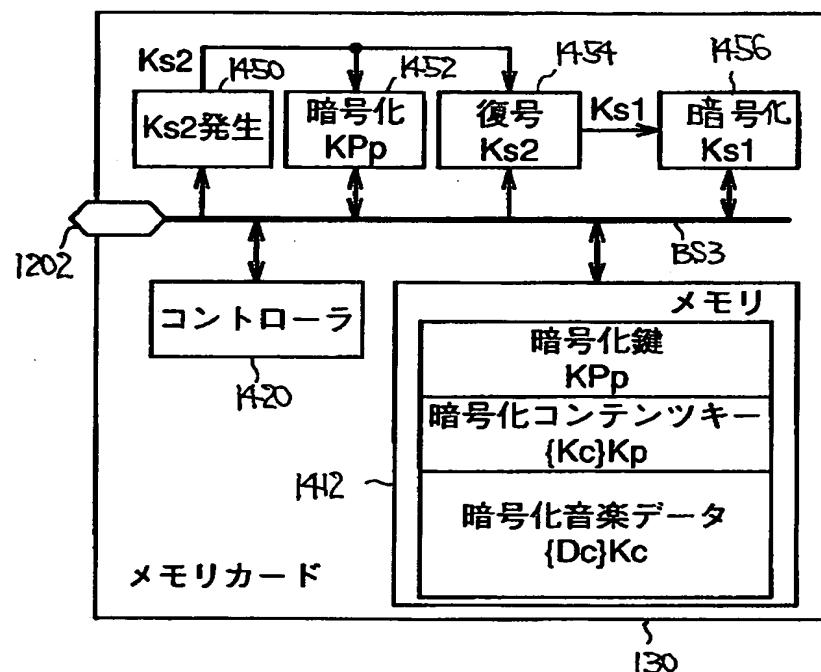


【図9】

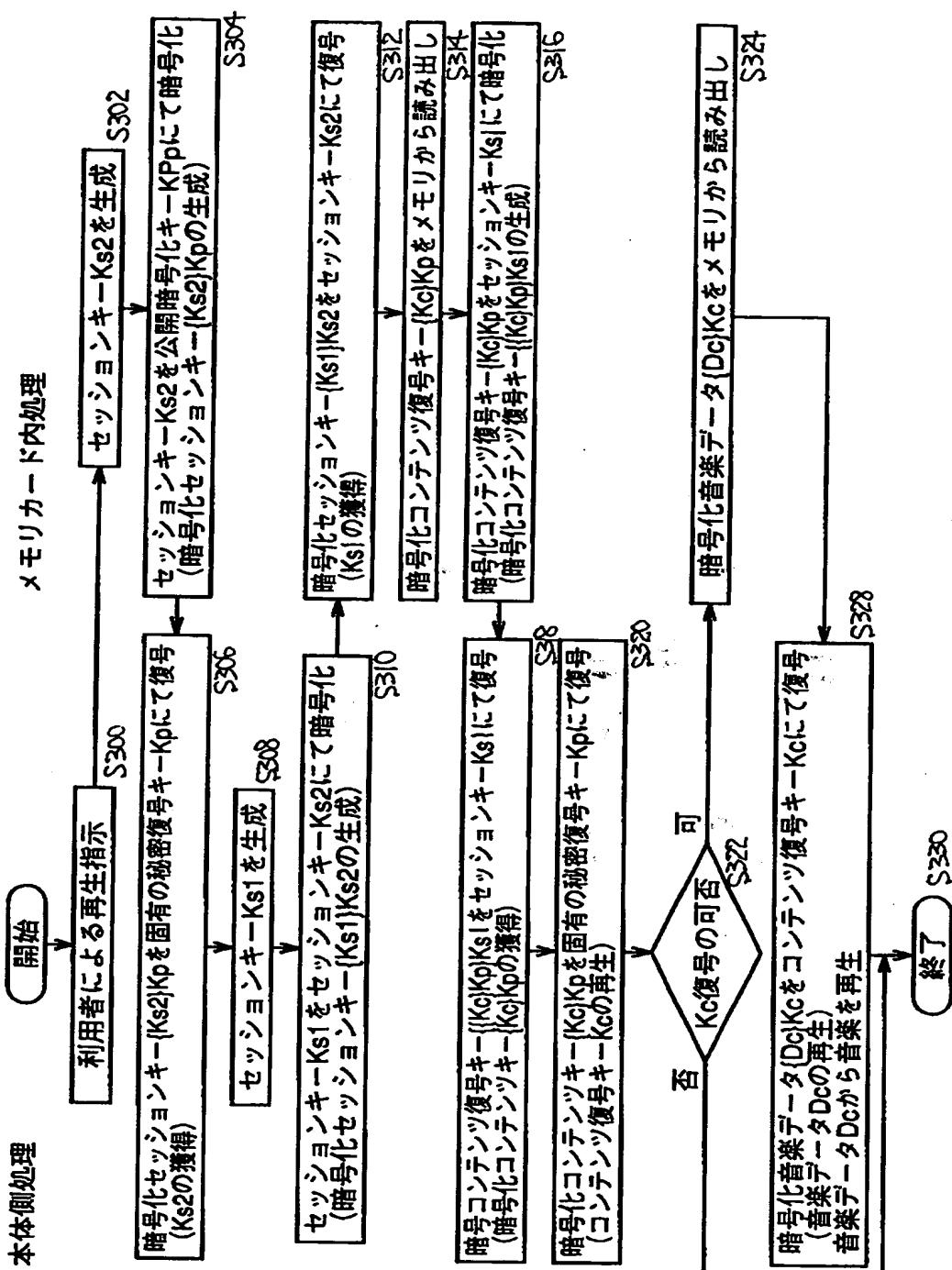
	記号	属性	特性
メモリカード 管理の鍵	Km	秘密復号鍵	メモリカード毎に異なる
	KPm	公開暗号鍵	KPmで暗号化されたデータは非対称な 復号鍵Kmで復号可能
音楽再生モジュール 管理の鍵	Ks2	共通鍵	セッション固有 メモリと音楽再生モジュール間 のアクセス毎に発生
	Kp	秘密復号鍵 (携帯電話機)	データ再生装置毎に異なる データ再生装置(携帯電話機)固有
配信データ	Ks1	共通鍵	セッション固有 メモリと音楽再生モジュール間 のアクセス毎に発生
	KPp	公開暗号鍵	KPpで暗号化されたデータは非対称な 復号鍵Kpで復号可能
	Kc	共通鍵	コンテンツキー 暗号化コンテンツデータの復号鍵
	Dc	コンテンツ データ	例: 音楽データ

【図10】

## メモリカード内の構造



【図11】



【書類名】 要約書

【要約】

【課題】 許可なく著作権物情報データにアクセスされることを防止することが可能なデータ再生装置を提供する。

【解決手段】 携帯電話機100は、配信された暗号化コンテンツデータおよび暗号化コンテンツキーをメモリ110に格納する。メモリ110から読み出された暗号化コンテンツキーデータは、K<sub>P</sub>保持部1540の保持するキーデータK<sub>P</sub>により復号処理部1530により復号されて、音楽再生モジュール1500に取り込まれる。復号処理部1520は、メモリ110から読み出した暗号化コンテンツデータを、復号処理部1530により抽出されたコンテンツキーK<sub>C</sub>により復号して、コンテンツデータD<sub>C</sub>を再生する。

【選択図】 図2

## 認定・付加情報

特許出願の番号	平成11年 特許願 第243583号
受付番号	59900838432
書類名	特許願
担当官	坪 政光 8844
作成日	平成11年 9月 3日

## &lt;認定情報・付加情報&gt;

## 【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号
【氏名又は名称】	富士通株式会社

## 【特許出願人】

【識別番号】	000004167
【住所又は居所】	東京都港区赤坂4丁目14番14号
【氏名又は名称】	日本コロムビア株式会社

## 【特許出願人】

【識別番号】	000001889
【住所又は居所】	大阪府守口市京阪本通2丁目5番5号
【氏名又は名称】	三洋電機株式会社

## 【代理人】

【識別番号】	100064746
【住所又は居所】	大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	深見 久郎

## 【選任した代理人】

【識別番号】	100085132
【住所又は居所】	大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	森田 俊雄

## 【選任した代理人】

【識別番号】	100091409
【住所又は居所】	大阪府大阪市北区南森町2-1-29 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	伊藤 英彦

## 【選任した代理人】

次頁有

認定・付加情報（続き）

【識別番号】 100096781  
【住所又は居所】 大阪府大阪市北区南森町2-1-29 住友銀行  
南森町ビル 深見特許事務所  
【氏名又は名称】 堀井 豊

次頁無

出願人履歴情報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号  
氏 名 富士通株式会社

出願人履歴情報

識別番号 [000004167]

1. 変更年月日 1990年 8月21日

[変更理由] 新規登録

住所 東京都港区赤坂4丁目14番14号  
氏名 日本コロムビア株式会社

出願人履歴情報

識別番号 [000001889]

1. 変更年月日 1993年10月20日

[変更理由] 住所変更

住 所 大阪府守口市京阪本通2丁目5番5号

氏 名 三洋電機株式会社